PROBLEMS OF CRIMINAL LAW OF THE RUSSIAN FEDERATION IN THE FIELD OF INFORMATION TECHNOLOGIES
KRIEVIJAS FEDERĀCIJAS KRIMINĀLLIKUMA PIELIETOJUMA PROBLĒMAS INFORMĀCIJAS TEHNOLOĢIJU JOMĀ

Vladimir Alekseenko
Pskov State University, v-ladimiralekseenko@yandex.ru, Pskov, Russia
Scientific supervisor: ***Elena Zykina*** *Candidate of Juridical Sciences, Associate Professor of the Pskov State University*

Abstract. *The purpose of this research is to find and consider the problems of the criminal law of the Russian Federation in the context of rapidly developing information technologies, as well as search and offer solutions to these problems. The problem of this research is that widespread information and computer technologies have generated many new illegal types of human activity, some of which are currently unsuccessfully regulated by the criminal legislation of the Russian Federation. The novelty of the research is justified by the novelty of the problem. The main conclusions of this research are suggestions of solutions to the problems considered on the further development of criminal law of the Russian Federation in the field of information and computer technologies.*
Keywords: *crime, criminal law, information technology, verdict.*

Introduction

The rapid development of information technology in the late 20th century led to the emergence of a new form of socially dangerous behaviour of the individual - cybercrime, the scale of which over the years just gets bigger. According to statistics, in 2017 the number of crimes in the field of information and telecommunication technologies increased from 65.949 to 90.587 *(Prosecutor General's Office of the Russian Federation, 2018).* Their share of all criminal acts registered in Russia is 4.4% - it is almost every 20th crime. The most frequent cybercrimes are illegal access to computer information (article 272 of the criminal code), creation, use and distribution of harmful computer programs (article 273 of the criminal code) *(The Criminal Code of the Russian Federation ,1996).*

Another consequence of global informatization has been a change in the face of crime in General, which has acquired new characteristics in connection with the use of information and communication technologies. The process of penetration of cybernetic methods, as well as tools of information and communication technologies in the mechanism of crime, actualizes the need to understand the condition and prospects of development of criminal law of the Russian Federation.

The purpose of the study is to consider the problems arising in the criminal code of the Russian Federation in connection with combating crimes committed using information and communication technologies. Now, modern society is faced with the need to solve the problem of building an effective system of information security and information and communication infrastructure; it is obvious that the solution to this problem requires the definition of a range of acts that infringe on information security, the counteraction of which must be effectively carried out through criminal law regulations.

Main body

Similar in nature, but qualitatively different group of acts from new forms of socially dangerous attacks on traditionally protected by criminal law social relations committed in the information environment *(Zhuravleva, 2014, p. 452).* A typical representative of this type is the theft of funds of the victim as a result of an automatic operation of the information system (widespread theft of funds from the Bank account through the use of remote banking services). An example, perhaps, also acts related to the requirement to transfer property as a condition of

 http://dx.doi.org/10.17770/iss2019.5272

unlocking the computer software, resuming access to e-mail or social network account, recovery of modified information.

Also, a much larger group is formed by traditional crimes, the objective side of which can be performed by means of software and hardware information processing. The peculiarity of these crimes is that in general, they do not require the use of methods or processes of information processing, but their Commission using information and computer technology is not only possible but also often encountered in practice *(Inogamova-Khegai, Komissarova, Rarog, 2008, p. 315).* Therefore, the use of a "site clone" or a fake electronic trading platform, sending messages to mobile phones, in which the intruder, posing as your relative, asks to transfer money to him are only new forms of deception as a traditional method of fraud.

Although the accumulated problems have made the changes not only necessary but also very late, at the moment it is difficult to imagine how much modern criminal code should change, adapting to the conditions of the information society. This is largely due to the lack or unreliability of criminological knowledge *(Babaev, Pudovochkin, 2014, p. 93).* This is clearly seen in the experience of criminalization of fraud in the field of computer information with the help of Art. 159.6 of the criminal code, which we want to regard in detail *(The Criminal Code of the Russian Federation ,1996).*

Currently, fraud has penetrated into all areas connected with property relations, including digital space. the classic form of this crime includes any acts that constitute theft of another's property or acquisition of the right to it by deception or abuse of trust. In April 2012, the Supreme Court of the Russian Federation submitted to the State Duma of the Federal Assembly a bill providing for the addition of a universal norm on fraud (article 159 of the criminal code) by a number of independent structures regulating the occurrence of criminal liability for fraud in various spheres of financial and economic activity *(Plenum of the Supreme Court of the Russian Federation, 2012).* Federal Law of November 29, 2012, №207-FZ Chapter 21 of the criminal code was supplemented with new articles providing for liability for fraud: in the field of lending (art. 159.1); upon receipt of payments (art. 159.2); using payment cards (art. 159.3); in the field of business (art. 159.4); in the field of insurance (art. 159.5); in the field of computer information (art.159.6). In the total numbers of articles providing for liability for various kinds of fraud, stands out article 159.6 of the criminal code, which protects several objects provided for by different chapters of the criminal code.

Now we should refer to the content of the explanatory note to the bill "About amendments to the criminal code of the Russian Federation and other legislative acts of the Russian Federation". In the document, the authors of the bill - representatives of the Supreme Court of the Russian Federation made a contradictory conclusion: "such crimes are not committed by deception or abuse of the trust of a particular entity, but by gaining access to a computer system and committing the above actions, which result in the theft of another's property or the acquisition of the right to another's property" *(Plenum of the Supreme Court of the Russian Federation, 2007).*

After analyzing this formulation, we concluded that there is a blurring of the concept of "fraud" in the wording of the disposition of Art. 159.6 of the criminal code. After all, it is generally accepted that "fraud" is theft by deception or abuse of trust; an act that has been assessed by the legislator as fraud is, in fact, a new form of theft. As a result, the validity of the criminalization of this act in an independent norm of the criminal code looks doubtful.

Analysis of the practice of application of the rule on "computer fraud" (Art. 159.6 of the criminal code) indicates the lack of uniformity in the qualification of such acts by the courts. So, the sentence of Grachevsky district court (Stavropol Krai) of June 13, 2013, N. was found guilty of a crime under part 1 of article 159.6 of the criminal code. N., having received on the mobile phone the electronic message by means of service "Mobile Bank" about the available limit of money on the Bank account which has not belonged to her opened in the name of S.,

was having intention to steal of the specified sum and realizing it, using the mobile phone belonging to her and the SIM card registered in the name of D. to which the service "Mobile Bank" of Sberbank of Russia providing the right to dispose of the money which are on the settlement account in the name of S is mistakenly connected by input of computer information in the form of electric signals - "SMS messages" on number "900", by means of a telecommunication network of the operator of cellular communication "Beeline" transferred the money which was on the settlement account of S., to the account belonging to N. SIM cards *(Grachevsky district court (Stavropol region) the verdict, 2013).*

Another legal assessment of a similar act was given by one of the district courts of Belgorod. C. received a message on the mobile phone number registered in his name, with the information of balance of the amount of money on the Bankcard, which was in use by an unknown person. Using the website of the cellular telephone company on the Internet, he transferred the amount of the balance of funds to the account of his SIM card, which he used for personal purposes. The verdict of Sverdlovsk district court of Belgorod of June 13, 2013. Found guilty of a crime under part 1 of article 158 of the criminal code (theft) *(Sverdlovsk district court of Belgorod (Belgorod region) the verdict, 2013, No 1-172/2013).* This discrepancy of verdicts on the part of the courts is due to the specifics of the subject and method of criminal assault.

So, the emergence of a special rule on fraud in the field of computer information had, in fact, the opposite effect, as it caused even more problematic issues. We consider the wording of article 159.6 of the criminal code controversial. Taking into account the specifics of the subject, method and means of Commission of the analyzed crimes, we propose to add another article in the criminal code of the Russian Federation about "Theft through the use of computer and information technologies", which would establish responsibility for theft of someone else's property or the right to property in favor of an attacker or third persons, if illegal interference in the functioning of means of storage, processing or transmission of computer information or information and telecommunication networks is used.

However, as an example of successful modernization of the criminal code to the conditions of informatization of crime can be an addition to the disposition of Art. 187 of the criminal code *(The Criminal Code of the Russian Federation ,1996)* such an alternative form of crime, as the manufacture, acquisition, storage, transportation for use or sale, as well as the sale of computer programs designed for the illegal implementation of the reception, issuance or transfer of funds.

Despite the scale and complexity of the problem of effective counteraction to crimes committed with the use of information and computer technologies, we believe that the modernization of Russian criminal law should be carried out very carefully, on the principle of minimizing the amendments. It should also be justified to identify the use of information and computer technology as an aggravated crime. Obviously, not every application of information technology (for example, the Internet) affects the degree of public danger of the deed. It does not matter if the disclosure of information constituting a commercial, tax or Bank secret has been made through the transfer of documents or by sending an e-mail. A fraudster who cheats victims through Facebook, ransomware who sends his threats through the Viber service, is unlikely to commit a more serious crime compared to its classical forms. So, the use of information and computer technologies is unequal in terms of the impact on the nature and degree of social danger of the crime. We adhere to this position and consider it the most rational, however, this issue is poorly developed in theory. Experts often skip this problem without relying on any criteria and almost intuitively suggest considering the use of information and computer technologies as the aggravated crime.

Conclusions and suggestions

We have explored some problems of criminal law of the Russian Federation in the field of information and computer technologies, studied and analyzed successful and unsuccessful decisions of the legislator, as well as the practice of their application and found, that despite the scale and complexity of the problem of effective combating crimes committed with the use of information and computer technologies, modernization of the Russian criminal code should be carried out very carefully on the principle of minimizing changes. We proposed a change to the criminal code by replacing art. 159.6.

We also concluded that the use of information and computer technologies is unequal in terms of impact on the nature and degree of public danger of the crime, and therefore it cannot always be considered an aggravating circumstance of the crime.

In conclusion, we add, that the legal problems associated with crimes committed with the use of information and computer technologies will eventually become more and more relevant. The rapidly developing information and communication infrastructure contain great potential for the development of jurisprudence, which is the key to the subsequent interest in this topic, including in the aspect of the science of criminal law.

Bibliography

1. *The Criminal Code of the Russian Federation* (1996, June 13). Law of the Russian Federation No 63-FL. Retrieved April 1, 2019 from http://www.consultant.ru/document/cons_doc_LAW_10699/
2. Babaev, M.M., Pudovochkin, Y.E. (2014). *Problems of Russian criminal policy*. Moscow: Prospekt. 327 p.
3. Grachevsky district court (Stavropol region) June 13, 2013 the verdict. Retrieved April 5, 2019 from https://sudact.ru/regular/doc/zEet1Kujky59/?regular-txt=&regular-case_doc=&regular-lawchunkinfo=&regular-doc_type=&regular-date_from=12.06.2013&regular-date_to=13.06.2013&regular-workflow_stage=&regular-area=1033&regular-
4. Inogamova-Khegai, L.V., Komissarova, V.S., Rarog, A.I. (2008). *Russian Criminal Law: Studies. for Universities: The Special Part*. (2nd ed.) Moscow: PROSPECT. 660 p.
5. Plenum of the Supreme Court of the Russian Federation (2007, December 27). *On Court Practice on Affairs about Fraud, Assignment and Waste*, Resolution No 51. Retrieved April 3, 2019 from http://www.consultant.ru/document/cons_doc_LAW_74060/
6. Plenum of the Supreme Court of the Russian Federation (2012, April 5). *On Entering into the State Duma of Federal Assembly of The Russian Federation of the Federal Law Draft "On Modification of the Criminal Code of the Russian Federation and Other Legal Acts of the Russian Federation"*, Resolution No 6. Retrieved April 2, 2019 from http://www.consultant.ru/cons/cgi/online.gi?req=doc;base=ARB001;n=269802#0645116213786967
7. Prosecutor General's Office of the Russian Federation (2018). *About Crimes Committed Using Modern Information and Communication Technologies*. Retrieved April 7, 2019, from http://genproc.gov.ru/smi/news/news-1431104/
8. Sverdlovsk district court of Belgorod (Belgorod region) June 13, 2013 the verdict No 1-172/2013. Retrieved April 4, 2019 from https://sudact.ru/regular/doc/Df4JwvB0beby/?regular-txt=&regular-case_doc=&regular-lawchunkinfo=&regular-doc_type=&regular-date_from=12.06.2013&regular-date_to=13.06.2013&regular-workflow_stage=&regular
9. Zhuravleva, M.P. Nikulin, S.I. (2014). *Criminal Law: General and Special Parts*. Moscow: Ltd "Legal publishing house Norma". 783 p.

Kopsavilkums

Raksts ir veltīts problemātiskiem Krievijas Federācijas krimināltiesību jautājumiem informācijas un datortehnoloģiju jomā, tai skaitā jautājumiem par to attīstības turpmākajām perspektīvām.

Tiek apzinātas galvenās informācijas vidē izdarīto noziegumu grupas, apskatīti gan veiksmīgi, gan neveiksmīgi likumdevēja lēmumi šajā jomā, kā arī ar to saistītā tiesu prakse, jautājums par informācijas un datortehnoloģiju izmantošanas atzīšanu par nozieguma kvalificējošu simptomu, kā arī informācijas un datora lietošanas ietekme. tehnoloģijas attiecībā

uz nozieguma veidu un tā bīstamību sabiedrībai. Izskatīts jautājums par informācijas un datortehnoloģiju izmantošanas atzīšanu par nozieguma kvalificējošu simptomu, kā arī par informācijas un datortehnoloģiju izmantošanas ietekmi uz nozieguma raksturu un sabiedriskās bīstamības pakāpi. Tika nolemts, ka Krievijas krimināltiesību modernizācija jāveic ārkārtīgi uzmanīgi, ievērojot grozījumu samazināšanas principu. Arī 159. panta 6. punkta redakcija tika uzskatīta par pretrunīgu un strīdīgu, tāpēc tika ierosināts ieviest vēl vienu Krimināl kodeksa pantu par "Zādzībām, izmantojot datoru un informācijas tehnoloģijas", kas noteiktu atbildību par cita īpašuma zādzību vai īpašuma tiesību atprasīšanu par labu uzbrucējam vai trešajām personām, ja tiek izmantota neatļauta iejaukšanās datoru informācijā vai telekomunikāciju tīklu informācijā tās glabāšanas, apstrādes vai pārsūtīšanas darbībā.

Sagatavojot rakstu, tika iegūti secinājumi un rezultāti, pamatojoties uz citu autoru viedokļu apkopojumu, juridisko avotu izvērtēšanu, tiesu prakses pētījumiem un informācijas monitoringu par reģistrēto noziegumu skaitu informācijas un datortehnoloģiju jomā.